**Verizon Communications**
1300 I Street NW, Suite 400W
Washington, DC 20005

Richard T. Ellis
Director – Federal Affairs

August 1, 2001

Ms. Magalie Roman Salas
Secretary
Federal Communication Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Verizon Communications CALEA Compliance Manual
CC Docket No. 97-213

Dear Ms. Salas:

Verizon respectfully submits its CALEA Compliance Manual for its wireline operations in accordance with Section 64.2105 of the Commission's Rules, 47 C.F.R. § 64.2105.

Should you have any questions with regard to this filing, please do not hesitate to contact me on 202-515-2534.

Sincerely,

cc: Mr. David O. Ward

# CALEA Compliance Manual for Verizon Communications

(Wireline Operations)

Filed with the Federal Communications Commission: August 1, 2001

## TABLE OF CONTENTS

APPENDIX I - Certification Form for Electronic Surveillance Implemented By **Verizon**

APPENDIX 2 - Relevant Federal Statutes

18 U.S.C. §§ 2510-2522 (Title III interceptions)
www.access.gpo.gov/uscode/title18/parti_chapter119_.html

18 U.S.C. §§ 3121-3127 (pen register and trap-and-trace surveillances)
www.access.gpo.gov/uscode/title18/partii_chapter206_.html

50 U.S.C. §§ 1801 -1811 (Foreign Intelligence Surveillance Act)
www.access.gpo.gov/uscode/title50/chapter36_subchapteri_.html

## I. DEFINTIONS

**Call content Interception** - an interception of a communication, including its content (*e.g.*, a wiretap carried out pursuant to a court order issued in accordance with Title III).

**Call information interception** - accessing dialing or signaling information that identifies the origin, direction, destination, or termination of a communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier (*e.g.*, a pen register or trap-and-trace surveillance).

**Electronic surveillance** - the implementation of either a call content interception or a call information interception.

**Title III** - Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which is the federal statute that sets minimum legal requirements for all call content interceptions by government officials and private citizens (except for those interceptions authorized under the Foreign Intelligence Surveillance Act). Title III is codified at 18 U.S.C. §§ 2510-2520.

## II. STATEMENT OF CORPORATE POLICY

It is the policy of Verizon to comply with the letter and spirit of all laws of the United States, including the Communications Assistance for Law Enforcement Act ("CALEA"). Section 105 of CALEA requires a telecommunication carrier to ensure, before assisting a law enforcement agency to carry out a call content interception or a call information interception, that the interception is activated (1) pursuant to court order or "other lawful authorization,"' and (2) with the "affirmative intervention" of a carrier officer or employee. 47 U.S.C. § 1004. The Federal Communications Commission has issued regulations to implement *section 105, see* 47 C.F.R. § 64.2100-2106, and these regulations require that carriers create policies and procedures to govern, their electronic surveillance activities. This Compliance Manual constitutes the required policies and procedures for Verizon.

All employees are required to follow the policies and procedures specified in this Manual. The FCC is authorized under CALEA to punish violations of both its regulations and carriers' internal surveillance policies. and procedures. In addition, Title 18 of the United States Code authorizes civil damages, fines, and imprisonment for the unlawful interception or disclosure of wire and electronic communications.

- Any questions about how to comply with the policies and procedures in this Manual should be referred to Verizon Director Electronic Surveillance or his/her designee at (800) 483-0722.

- Any violation of or departure from the policies and procedures in this Manual should be reported immediately to Verizon Director Electronic Surveillance or his/her designee at (800) 483-0722.

## III. GENERAL POLICIES FOR ELECTRONIC SURVEILLANCE

### A. "Appropriate Authorization" Required To Conduct Electronic Surveillance

It is the policy of Verizon to permit only lawful, authorized electronic surveillance to be conducted on its premises.

Employees shall have both "appropriate legal authorization" and "appropriate carrier authorization" before enabling law enforcement officials and carrier personnel to implement the interception of communications or to access call-identifying information. Section IV of this Compliance Manual sets forth how each form of authorization is to be obtained.

### B. Employees Designated as Points of Contact

Verizon hereby designates the Security Director Electronic Surveillance or his/her designee to act as the primary point of contact for law enforcement agencies that wish to conduct electronic surveillance. The Security Director Electronic Surveillance or his/her designee shall be available to law enforcement agencies 24 hour a day, 7 days a week and may be contacted at (800) 483-0722, 24 hours a day, 7 day a week

## C. Job Description for Designated Employees

1. The employees designated in Section IIIB above are hereby authorized by Verizon to implement lawful electronic surveillance in accordance with the policies and procedures in this Manual and to delegate any tasks associated with the surveillance to other employees.

2. An employee designated in Section III.B above shall:

   - Oversee the implementation of each electronic surveillance conducted on the premises of Verizon;

   - Be responsible for assuring that he/she is fully apprised of all relevant state and federal statutory provisions affecting the legal authorization a carrier must have to conduct electronic surveillance, including section 2518(7) of Title 18 of the United States Code, which authorizes certain law enforcement personnel to conduct the interception of communications without a court order if an emergency situation exists involving:

     (i) immediate danger of death or serious physical injury to any person,

     (ii) conspiratorial activities threatening the national security interest, of

     (iii) conspiratorial activities characteristic of organized crime.

     **(NOTE: The relevant federal statutory provisions are attached as Appendix 2, and procedures for compliance with them are set forth in Section IV of this Manual.**

   - Affirmatively intervene to ensure that there is appropriate legal authorization for each electronic surveillance, including any appropriate authorization required under relevant state and f6deral statutes;

   - Complete a certification form for each (ii) electronic surveillance (above) he/she oversees and do so either contemporaneously with or within a reasonable period of time after the initiation of, the surveillance.

   - Ensure that all available records for each surveillance are placed in the appropriated files.

3. Security Director Electronic Surveillance shall ensure that this manual is updated and filed with the FCC within 90 days of any amendment or Verizon's merger with another company.

## D. Recordkeeping

Security Director Electronic Surveillance or his/her designee shall complete a Certification Form (model attached as Appendix 1) for *every* authorized electronic surveillance conducted on carrier premises.

Security Director Electronic Surveillance or his/her designee shall establish and label separate files in which it will retain all certification forms, court orders, and other records for **(1) authorized call content interceptions;** and **(2) authorized call information interceptions.** These records shall be retained in secure and appropriately marked files for a time period of 10 years from the time the Certification Form is completed for the interception. It has been the custom and policy of Verizon to maintain these records for this period of time, and experience has shown that this policy has adequately served the needs of Verizon and law enforcement agencies.

## E. Unauthorized Surveillance and Compromises of Authorized Surveillance

Employees are prohibited from conducting any unauthorized surveillance and from disclosing to any person the existence of, or information about, any law enforcement investigation or electronic surveillance unless required by legal process and then only after prior notification to a representative of the Attorney General of the United States or to the principal prosecuting attorney of the state or subdivision thereof, as may be appropriate.

Employees shall report any incidents of unauthorized surveillance and any compromises of authorized surveillance in accordance with the procedures in Section V of this Manual.

## IV. PROCEDURES FOR THE CONDUCT OF AUTHORIZED SURVEILLANCE

### A. Call Content Interceptions *with* a Title III Court Order

Step One. Any court order presented by a law enforcement agency for a call content interception pursuant to Title III shall be referred immediately to one of the employees designated in Section III.B of this Manual.

Step Two. Before implementing the interception, the designated employee shall ensure that the court order contains the following information:

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities or the place for which authority to intercept is granted;

(c) a particular description of the type of communications sought to be intercepted and a statement of the particular offense to which it relates;

(d) the period of time during which the interception is authorized, including a statement whether the, interception shall automatically terminate when the described communication has been first obtained;

(e) a provision that the authorization to intercept shall be executed as soon as practicable and conducted in such a way as to minimize the interception of communications not otherwise subject to interception; AND

(f) the signature of a judge or magistrate.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply a information requested on the Certification Form that is not contained-on the court order. The employee then shall attach the court order to the Certificate Form and sign the Certification Form. The employee also shall attach to the Certification Form any extensions that are granted for the surveillance.

Step Six. The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the court order (which, in the absence of an extension, cannot exceed 30 days).

### B. Call Content Interceptions Pursuant to Title III but *without* a Court Order

Step One. Any request by a law enforcement agency for a call content interception without a court order, pursuant to the exigent circumstances listed in 18 U.S.C. § 2518(7), shall be referred immediately to one of the employees designated in Section III.B of this Manual.

Step Two. Before implementing the interception, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information:

(a) the information, facilities, or technical assistance required;

(b) the period of time during which the provision of information, facilities, or technical assistance is authorized;

(c) a statement that no warrant or court order is required by law;

(d) a statement that all statutory requirements have been met;

(e) a statement that the specific requested assistance is required; AND

(f) the signature of *either* (i) the Attorney General of the United States, *or* (ii) a law enforcement officer specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six. The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur.

(a) the law enforcement agency does not apply for a court order within 48 hours after the interception has begun; or

(b) the law enforcement agency's application for a court order is denied.

Step Eight. If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.A, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.A.

### C. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device *with* a Court Order

Step One. Any court order presented by a law enforcement agency for a call information interception using a pen register or trap-and-trace device shall be referred immediately to one of the employees designated in Section III.B of this Manual.

Step Two. Before implementing the interception, the designated employee shall determine that the court order contains the following information:

(a) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap-and-trace device is to be attached;

(b) the identity, if known, of the person who is the subject of the criminal investigation;

(c) the number and, if known, physical location of the telephone line to which the pen register or trap-and-trace device is to be attached and, in the case of a trap and-trace device, the geographical limits of the trap-and-trace order,

(d) a statement of the offense to which the information likely to be obtained by the pen register or trap-and-trace device relates; AND

(e) the signature of a judge or magistrate.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that arc granted for the surveillance.

Step Six The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The designated employee shall terminate the surveillance at the time specified in the order (which, in the absence of an extension, cannot exceed 60 days).

## D. Call Information Interceptions Using a Pen Register or Trap-and-Trace Device *without* a Court Order

Step One. Any request for a call information interception using a pen register or trap-and trace device without a court order shall be referred immediately to one of the employees designated in Section III.B of this Manual.

Step Two. Although the federal statute does not expressly require a certification in these circumstances, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request:

(a) the information, facilities, or technical assistance required;

(b) the period of time during which the provision of information, facilities, or technical assistance is authorized;

(c) a statement that no warrant or court order is required by law;

(d) a statement that all statutory requirements have been met;

(e) a statement that the specific requested assistance is required; AND

(f) the signature of a law enforcement officer specially designated by the Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any state or subdivision thereof.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six. The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur:

(a) the information sought is obtained;

(b) the law enforcement agency's application for the court order is denied; or

(c) 48 hours have lapsed since the installation of the device without the granting of a court order.

Step Eight. If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court Order (as specified in Section IV.C, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.C.

## E. Electronic Surveillance Pursuant to the Foreign Intelligence Surveillance Act ("FISA") *with a* Court Order

Step One. Any court order presented by a law enforcement agency for electronic surveillance pursuant to FISA shall be referred immediately to one of the employees designated in Section M.B of this Manual.

Step Two. Before implementing the interception, the designated employee shall ensure that the court order contains the following information:

(a) the identity, if known, or a description of the target of the electronic surveillance;

(b) the nature and location of each of the facilities or places at which the electronic surveillance will be directed;

(c) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(d) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance;

(e) the period of time during which the electronic surveillance is approved;

(f) whenever more than one electronic, mechanical, or other surveillance device is to be used under the order, the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device;

(g) a statement directing that the minimization procedures be followed;

(h) a statement directing that, upon the request of the applicant, a specified carrier furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that the carrier is providing that target of electronic surveillance;

(i) a statement directing that the carrier maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain;

(j) a statement directing that the applicant compensate, at the prevailing rate, the carrier for furnishing the aid; AND

(k) the signature of a federal district judge.

Whenever the target of the electronic surveillance is a foreign power (as defined under FISA) and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the court order need not contain the information required by subparagraphs (c), (d), and (f), but shall generally describe the information sought, the communications or activities to be subjected. to the surveillance, and the type of electronic surveillance involved, including whether physical entry is required.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the court order is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four. The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply all information requested on the Certification Form that is not contained on the court order. The employee then shall attach the court order and sign the Certification Form. The employee also shall attach any extensions that are granted for the surveillance.

Step Six. The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee shall continue to oversee the conduct of the electronic surveillance and ensure that the surveillance terminates when the legal authorization expires. The interception shall be terminated at the time specified in the order. In the absence of an extension, the surveillance cannot exceed 90 days (or 1 year if the surveillance is targeted against a foreign power).

## F. Electronic Surveillance Conducted Pursuant to FISA *without* a Court Order

Step One. Any request by a law enforcement agency for electronic surveillance pursuant to FISA but without a court order shall be referred immediately to one of the employees designated in Section III.B of this Manual.

Step Two. Although FISA does not expressly require a certification in these circumstances, the designated employee shall ensure that the law enforcement agency provides a certification containing the following information before implementing the request:

(a) the information, facilities, or technical assistance required;

(b) the period of time during which the provision of information, facilities, or technical assistance is authorized;

(c) a statement that no warrant or court order is required by law;

(d) a statement that all statutory requirements have been met;

(e) a statement that the specific requested assistance is required; AND

(f) the signature of *either* (i) the Attorney General of the United States, *or* (ii) a law enforcement officer specially designated by the Attorney General.

Step Three. The designated employee also shall determine whether the surveillance can be implemented technically AND whether the certification is sufficiently and accurately detailed to enable the carrier to comply with its terms.

Step Four The designated employee may implement the surveillance and may delegate tasks associated with the surveillance to other employees, but the designated employee shall continue to oversee the implementation of the surveillance.

Step Five. The designated employee shall complete a Certification Form (attached as Appendix 1) as soon as possible after the initiation of the electronic surveillance. The employee shall supply all information requested on the Certification Form that is not contained on' the certification provided by the law enforcement agency. The employee then shall attach the certification provided by the law enforcement agency and sign the Certification Form.

Step Six. The designated employee shall ensure that the Certification Form is placed in the appropriate file.

Step Seven. The designated employee, shall continue to oversee the conduct of the electronic surveillance and terminate the surveillance as soon as any of the following events occur;

(a) the information sought is obtained;

(b) the law enforcement agency's application for a court order is denied; or

(c) 24 hours have elapsed since the authorization of the surveillance by the Attorney General without the granting of a court order.

Step Eight. If the law enforcement agency does receive a court order for the surveillance, the designated employee shall validate the court order (as specified in Section IV.E, Step Two above), attach the order to the Certification form, and handle the surveillance in all respects under the procedures in Section IV.E.

## V. PROCEDURES IF UNAUTHORIZED SURVEILLANCE OR A COMPROMISE OF SURVEILLANCE HAS OCCURRED

Step One. If any employee becomes aware of any act of unauthorized electronic surveillance or any compromise of authorized surveillance to unauthorized persons or entities, that employee shall report the incident immediately to one of the employees designated in Section III.B of this Manual.

Step Two. The designated employee shall promptly notify Verizon Director Electronic Surveillance of the incident. Acting with legal counsel, the designated employee and Verizon Director Electronic Surveillance shall determine which law enforcement agencies are affected and promptly notify the agencies of the incident.

Step Three. The designated employee shall compile a certification record for any unauthorized surveillance and ensure that all records available to the carrier regarding the surveillance are placed in the appropriate carrier files.

## APPENDIX 1

Certification Form for Electronic Surveillance Implemented By Verizon

INSTRUCTIONS: The information requested below shall be provided either on this form or by attaching the appropriate legal authorization for the surveillance if the authorization contains that information. If the authorization is attached, check the box below and attach any extensions that are granted for the surveillance.

_____ I have attached the court order or other legal authorization for this surveillance as well as any extensions that have been granted.

**CONTROL NUMBER**_____

| | |
|---|---|
| 1. Telephone number(s) and/or circuit identification numbers involved | |
| 2. Start date and time of the opening of the circuit for law enforcement | |
| 3. Law enforcement officer presenting the authorization | |
| 4. Person signing the appropriate legal authorization | |
| 5. Type of surveillance (e.g., pen register, trap and trace, Title III, FISA) | |
| 6. Carrier employee who is responsible for overseeing the surveillance | |

I_____, have overseen the electronic surveillance described on this form and on any attached documents, and I hereby certify that the information contained on this form and the attached documents is complete and accurate.

Signed:_____

Date:_____